



Department of Homeland Security Daily Open Source Infrastructure Report for 06 November 2006

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- The Seattle Times reports Starbucks said on Friday, November 3, that personal data on 60,000 present and former employees and contractors was on two laptop computers missing from its Seattle headquarters. (See item [8](#))
- The FBI has arrested more than a dozen people in the U.S. and other countries in an international identity theft operation — called Operation Cardkeeper — that involves the trading of social security numbers, the sale of stolen credit card account information, and phishing. (See item [10](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *November 05, International News (UK)* — **Cold weather triggers massive electricity blackout across Europe.** A surge in electricity demand in Germany due to cold weather triggered massive blackouts across western Europe on Saturday, November 4, including to about a tenth of France, electricity operators said. About five million consumers lost power in the blackout, and similar cuts occurred in all Western European countries. The German energy company RWE said the blackouts were caused by surging electricity demand Saturday evening due to a plunge in temperatures to the freezing point. Insufficient electricity supply first

triggered blackouts in parts of western Germany, particularly in Cologne, and then across France. Electricity was then knocked out in parts of Paris and its suburbs, as well as numerous other areas of France. The blackout also disrupted the country's high-speed trains, causing delays on a dozen lines, the SNCF train company said. Various parts of Italy were also affected, particularly the northwestern Piedmont area, which lost electricity for around 30 minutes.

Source: http://www.thenews.com.pk/update_detail.asp?id=12376

2. *November 04, New Mexican* — **Lab: Classified files not most sensitive.** Most of the classified material found recently at the home of a former Los Alamos National Laboratory contract employee was low level and decades old, and none of it was top secret, the lab said Friday, November 3. However, some of the classified information was of "moderate" importance, a lab spokesperson said. The FBI is investigating the security breach at the lab, but no arrests have been made since it got involved in the case October 20. The lab has confirmed classified material was found in the home of a former contract employee. The woman at the center of the investigation had an extremely high security clearance and access to extremely sensitive information. Santa Fe defense lawyer Steve Aarons has confirmed 22-year-old Jessica Quintana is being investigated by the FBI. Aarons has described her as an overworked archivist trying to meet a deadline to convert hard copies of documents into electronic form. He said about 200 pages of hard copy documents were found at her home as well as a computer flash drive with roughly the same number of pages. Aarons maintains national security was not compromised.

Source: <http://www.freewmexican.com/news/51621.html>

3. *November 04, Times (IN)* — **Fear may have lead to increase in oil prices in wake of bomb threat at refinery.** A bomb threat Friday morning, November 3, at a Whiting, IL, BP Refinery was an apparent hoax, but the incident likely helped cause a spike in U.S. oil prices as traders feared a gasoline supply disruption. Agents from the U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives and FBI helped Whiting and East Chicago officers search two units of the refinery in response to a threatening phone call made to the refinery by an unidentified person, refinery spokesperson Thomas Keilman said. About 200 "nonessential" employees and contractors were evacuated in response to the call at the 1,200-employee refinery. Although he declined to reveal the nature of the threat, Keilman said the call specifically mentioned two refinery units: the Cat Cracker, a major gasoline production unit, and the alkylation unit, where gasoline's octane is upgraded. The two units are in close proximity to each other amid the refinery's 1,600 acres that span Whiting and East Chicago. News of the threat and the resulting evacuation may have been among the causes for U.S. light sweet crude oil prices to rise early Friday because of the possibility the refinery's supply of gasoline could have been disrupted, according to reports from Wall Street.

Source: http://www.thetimesonline.com/articles/2006/11/04/news/top_news/007c38e8f674a7768625721c00025dcd.txt

4. *November 02, Chicago Sun-Times* — **Man mistakes nuclear power plant for gas station.** A highly intoxicated man faces several charges after driving up to the Braidwood, IL, nuclear power plant in search of gasoline Saturday, October 28, police said. The incident was the second time in two weeks that a drunken motorist mistakenly pulled up to a security checkpoint at the Braidwood Generating Station. The nuclear power plant is about 60 miles southwest of Chicago. On October 18, a 38-year-old man drove in and tried to pay a guard, thinking he was

at an interstate toll plaza. Krista Lopykinski, a spokesperson for plant owner Exelon, said the two incidents were "unusual" but that the plant's security force handled them properly. About 12:30 a.m. CDT Saturday, Stanislaw Drobrzawski steered his 2000 Ford Explorer past "No Trespassing" and a 10-foot-wide "Braidwood Generating Station" sign, stopping only when he reached a security checkpoint. "He thought it was a gas station — I guess he wanted to pay for gas," said Will County sheriff's office spokesperson Pat Barry.

Source: http://cbs2chicago.com/local/local_story_306112332.html

5. *November 02, USA TODAY* — **Faulty equipment, poor air flow cited in deaths of two coal miners.** State investigators said missing walls to control air flow and faulty firefighting equipment were key factors in the deaths of two miners in a conveyor belt fire at a West Virginia coal mine in January. Investigators concluded that the missing walls allowed smoke to enter the main escape route at Massey Energy Co.'s Aracoma Alma No. 1 Mine in Logan County, the West Virginia Office of Miners' Health, Safety and Training said Thursday, November 2. The agency also determined that the mine was not following its approved ventilation plan. Air that should have gone to the face of the coal seam was being pumped in the opposite direction. Water lines for fire hoses and sprinklers at the scene of the fire were shut off and fire hoses at the site couldn't be connected because of incompatible fittings, a problem that had been reported to management after a similar fire December 23. Investigators said the January 19 fire resulted from a misaligned conveyor belt that carries coal. Mine personnel could not fix the alignment problem before the evening shift started, but they operated the belt anyway, the report said.

Source: http://www.usatoday.com/news/nation/2006-11-02-coal-miners_x.htm

6. *November 02, Associated Press* — **Japanese nuke plant produces test fuel.** A nuclear reprocessing plant seen as key to Japan's efforts to reduce its reliance on energy imports produced its first batch of the solution necessary for making fuel during a test-run, Japan Nuclear Fuel spokesperson Shigehiro Ito said Thursday, November 1. The Rokkasho fast-breeder reactor produced its first batch of MOX solution, which can eventually be turned into a powder that is the basic ingredient necessary for fuel production, Ito said. Fast-breeder reactors are central to resource-poor Japan's plans to reduce its dependency on energy imports. The reactors produce more plutonium faster than traditional electricity-generating reactors, which is then turned into MOX fuel. Japan, which now relies on nuclear plants for a third of its energy needs, aims to raise that to nearly 40 percent by 2010. It plans to convert 18 electricity-generating plants to fast-breeder reactors. The Japanese public has grown increasingly wary of the nuclear power industry following a spate of safety problems, shutdowns, and cover-ups. Safety problems have also left Japan's nuclear fuel-cycle program in a shambles. The country's first experimental fast-breeder reactor was ordered permanently shut down after more than a ton of volatile liquid sodium leaked in 1995.

Source: http://biz.yahoo.com/ap/061102/apfn_japan_nuclear_power.html?v=1

[[Return to top](#)]

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[[Return to top](#)]

Defense Industrial Base Sector

Nothing to report.

[\[Return to top\]](#)

Banking and Finance Sector

7. *November 05, Agence France–Press* — **Spain freezes two billion dollars in tax fraud probe.**

Spanish police said that \$2.3 billion dollars had been frozen in bank accounts as investigations continued into possible tax fraud. Several banks were searched Thursday, November 2. Police and the national fraud investigation office (ONIF) said they "detect[ed] a tax fraud which could involve many bank accounts." A branch of the Portuguese Banco Espirito Santo on the Portuguese island of Madeira is suspected of setting up "companies aimed at hiding the origin and ownership of large sums of money deposited in Spain in non–resident accounts," ONIF said. As part of the investigation five searches were conducted in Madrid and six in the Catalan capital Barcelona in the offices of the Espirito Santo bank, the French bank BNP Paribas, and the headquarters of the Cahispa Seguros insurance company. "The funds were leaving Spain through a network of accounts whose holders were of the 'trust' type set up in Madeira and other countries," the police said. Subsequently "the money was undoubtedly sent to other foreign accounts and finally returning to accounts in Spain via Luxembourg", the police said.

Source: <http://www.todayonline.com/articles/152688print.asp>

8. *November 04, Seattle Times* — **Missing Starbucks laptops had data on 60,000 employees, contractors.** Starbucks said Friday, November 3, that personal data on 60,000 present and former employees and contractors was on two laptop computers missing from its Seattle headquarters. A Starbucks employee realized in September that four laptops in a closet were gone. Only two contained personal data, including names, addresses, and Social Security numbers. A two–month investigation did not turn up the computers, so this week Starbucks sent letters to the last known addresses of all 60,000 people. The data on the laptops was password–protected. "We aren't convinced they're in the hands of someone who intends to misuse the information," spokesperson Valerie O'Neil said. Starbucks has contacted the police and is updating procedures around the protection of personal data. The people whose data is missing began working for Starbucks before December 31, 2003. Most of them worked in the United States, and a few in Canada.

Source: http://seattletimes.nwsourc.com/html/localnews/2003344677_s_starbucks04.html

9. *November 04, Philadelphia Inquirer* — **Did bank stop a fraud or terrorist?** It could be identity theft. It could be money laundering. Or, it could be terrorism. On Wednesday morning, November 1, two men withdrew \$8,700 from an account under the name of Shahid Batti at the Commerce Bank on Garrett Road in Upper Darby, PA. When they returned later in the day to withdraw an additional \$9,700, bank officials became suspicious and contacted police. The two men were stopped by police. One man produced a passport from Pakistan, a New Jersey license, and a Social Security card, all under the name of Batti — and all fraudulent, according to police. The second man, who was acting as a driver, was released and not charged. During questioning, the man who carried the identification and credit and bank cards identified himself

as Raza Hussain from Brooklyn, NY. During their investigation, police discovered a "possible" connection between Hussain and a terrorist with the same birthday when they ran the names through the FBI Terrorism Screening Center. He said the FBI and the New York Police Department have been contacted. Police said the address on the bank account was for Batti Trading in the 6400 block of Market Street, which was a vacant building.

Source: http://www.philly.com/mld/inquirer/news/local/states/pennsylvania/counties/bucks_county/15925991.htm?source=rss&channel=inquirer_bucks_county

10. *November 03, Washington Post* — **FBI tightens net around identity theft operations.** The FBI is cracking down on an international identity theft operation that involves the trading of social security numbers; the sale of stolen credit card account information; and phishing, authorities said Thursday, November 2. Called Operation Cardkeeper, the investigation has brought about the arrests of more than a dozen people in the U.S. and other countries who are members of online communities that specialize in "carding," the trafficking of stolen identities and credit card and bank account information. Investigators said some members of the criminal rings purchased data that was electronically copied from the magnetic strip on the back of credit or debit cards and used the information to create counterfeit cards for cash withdrawals and retail purchases. Others sold Social Security numbers and other personal data through online carder forums. That data was later used to obtain credit cards in the victims' names. Facing charges or search warrants in the U.S. are people from Ohio, Georgia, New York, Texas, Tennessee, and Nebraska. The FBI also assisted in the arrests of 11 people in Poland believed to be connected to a network of online fraud forums.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/11/02/AR2006110201579.html>

11. *November 02, TechWeb* — **Survey: Consumers less concerned about online security.** Consumer trust in online transactions is up, according to a survey published Thursday, November 2, which found that Americans are less concerned about online security now than they were two years ago. The survey, conducted by Lieberman Research, said that the percentage of people who don't trust the Internet with the security of their financial information dropped to eight percent in 2006 from 20 percent in 2004. Meanwhile, the number of those who believe that paying bills online is safer than using paper checks increased during the same period. James Van Dyke of Javelin Strategy & Research said that fear of the Internet based on the threat of identity theft is "flattening and leveling off," largely due to increased security by banks, online brokers, and electronic retailers. The survey also showed that Americans are increasingly abandoning paper. From 2004 to 2006, the percentage of people who said they preferred to handle finances with a traditional paper-based approach dropped from 22 percent to nine percent. "People are starting to realize that the Internet is one of the best ways to reduce your risk of identity fraud," said Van Dyke. Users are more closely monitoring their accounts, and doing that predominantly online.

Source: <http://www.techweb.com/wire/security/193501387;jsessionid=KIQLDFELX4OTAQSNDLOSKH0CJUNN2JVN>

12. *November 02, Miami Herald (FL)* — **Seven charged in fuel-skimming thefts in Florida.** Seven South Florida men are charged with skimming fuel delivered at Port Everglades in Fort Lauderdale, FL, for their own personal and business vehicles, the Federal Department of Immigration and Customs Enforcement announced Wednesday, November 1. Over a period of

months, the men stole more than 11,000 gallons from companies getting fuel delivered at the port. The men worked for Genesis Petroleum which operated tanker trucks that hauled gasoline and diesel fuel to customers. Genesis drivers would go to a private lot near the port and deliver fuel for themselves inside a 40–inch shipping container. The investigation revealed that fuel was loaded into two storage tanks inside the container; the container itself violated fuel storage safety regulations. After the deposits, the fuel was used to fill up work trucks, personal vehicles, and gas containers belonging to Genesis employees, their relatives, and friends.

Source: http://www.miami.com/mld/miamiherald/news/local/states/florida/counties/broward_county/15906573.htm?source=rss&channel=miamiherald_broward_county

[[Return to top](#)]

Transportation and Border Security Sector

13. *November 03, Associated Press* — **Half of runways don't have safety zone.** More than half of U.S. commercial airports don't have a 1,000–foot margin at the end of a runway, an overrun area the federal government says is needed as a safety zone, according to a new report. Some of the busiest airports in the country — including Los Angeles International Airport, Chicago's O'Hare International Airport, and Hartsfield–Jackson Atlanta International Airport — have more than one runway that doesn't meet safety standards, according to statistics supplied by the Federal Aviation Administration (FAA). The FAA says it is diligently upgrading the runways. The agency expects that all of them will meet the standard by 2015, when they are legally required to do so, according to FAA spokesperson Laura Brown. Deadly airplane crashes can happen on runways because they're too short, improperly lit, poorly designed or lack safety equipment. A minor procedural error by a pilot or an air traffic controller can turn tragic if a vehicle or another airplane happens to be in the way. Federal safety investigators are looking into three runway mishaps this week alone: An Alaska Airlines jet landed on the wrong runway at Seattle–Tacoma International Airport; two airliners clipped wings while taxiing at Newark Liberty International Airport; and another jet landed on a taxiway at Newark.

Source: <http://www.cnn.com/2006/US/11/03/runway.safety.ap/index.html>

14. *November 03, New York Times* — **FAA finds more errors on runways.** The National Transportation Safety Board lists protection against “runway incursion” as a “most wanted” safety improvement, and has declared unacceptable the Federal Aviation Administration’s (FAA) responses to its previous recommendations on that subject. Runway incursion occurs when a plane, a vehicle, or a pedestrian strays onto a runway that has been assigned for use by another plane. The problem becomes more serious as the number of takeoffs and landings increases. Hardware already on airliners could be used to make it harder for crews to pick the wrong runway but has been used only on wide–body jets. Airliners already carry a system that uses global positioning to warn pilots if they are too close to the ground or heading into a mountain. There is a software upgrade that makes the system announce, in a mechanical voice, which runway the plane is on. This system knows what kind of plane it is installed on, and its approximate required length for takeoff. If the runway is too short, the system makes announcements like “3,000 feet remaining,” as a warning. But the system costs about \$18,000 per plane, and the FAA does not require it.

Source: <http://www.nytimes.com/2006/11/03/us/03runway.html? r=1&ref= us&oref=slogin>

15. *November 03, Associated Press* — **Washington, DC rails getting electronic security.** Rail tracks in the District are getting an electronic security perimeter to monitor unauthorized people and hazardous material. The National Capital Planning Commission passed a \$10 million pilot plan on Thursday, November 2, for the state-of-the-art system. The plan includes video surveillance cameras and chemical detectors on an eight-mile section of the freight and commuter tracks.
Source: http://www.wusatv9.com/news/news_article.aspx?storyid=53284
16. *November 03, Associated Press* — **Malaysia Airlines plane loses engine parts in takeoff.** A Malaysia Airlines jet with 300 people on board lost several engine parts during takeoff Friday, November 3, forcing it to return to a Swedish airport, officials said. The Boeing 777, which was headed to Kuala Lumpur, turned around after dumping fuel and landed safely at Stockholm's Arlanda airport, spokesperson Niclas Harenstam said. No one was injured. Harenstam said several engine parts from the plane fell off during takeoff and ended up in the grass next to the runway. "Losing parts of the engine is highly unusual, I've never seen that before," Harenstam said. "A plane can actually fly as well on one engine as with two, but you don't really want to fly to Kuala Lumpur on one engine."
Source: http://www.usatoday.com/travel/flights/2006-11-03-plane-loses-engine-parts_x.htm
17. *November 03, Los Angeles Times* — **Ports get mobile radiation detectors.** In the effort to protect the nation's busiest harbor from terrorist attack, federal officials announced Thursday, November 2, the addition of 18 mobile radiation detectors in the ports of Los Angeles and Long Beach. The devices, which will check cargo containers on ships, trucks and trains, are part of a group of 24 portable scanners that will be delivered by January. U.S. Customs and Border Protection officials say the monitors will supplement 85 stationary radiation detectors that have been used at 14 port terminals since June 2005. The devices scan shipping containers for nuclear materials as trucks leave the harbor. In addition, customs officers use small hand-held detectors on the docks and wharves to check cargo as it is unloaded from ships.
Source: <http://www.latimes.com/news/printedition/california/la-me-scanners3nov03.1,2818477.story?coll=la-headlines-pe-california&ctrack=1&cset=true>
18. *November 03, Associated Press* — **Texas puts 'virtual border watch' online.** Texas has started broadcasting live images of the U.S. border on the Internet in a security program that asks the public to report signs of illegal immigration or drug crimes. A test Website went live Thursday, November 2, with views from eight cameras and ways for viewers to e-mail reports of suspicious activity. Previously, the images had only been available to law enforcement and landowners where the cameras are located. The cameras will operate at hot spots for illegal activity, such as Amistad Reservoir in Del Rio and Falcon Lake in Zapata, and other active border areas such as highway rest stops and inspection stations,
Website: <http://www.texasborderwatch.com>
Source: http://news.yahoo.com/s/ap/20061103/ap_on_re_us/border_cameras_1

[[Return to top](#)]

Postal and Shipping Sector

19. *November 03, Associated Press* — **FedEx increasing rates.** FedEx Express, the largest business unit of the FedEx Corps, will increase net average shipping rates by 3.5 percent at the beginning of the year, the company announced Friday, November 3. The rate change will be made up of a 5.5 percent increase in standard list rates and a two–percentage point reduction in fuel surcharges, the Memphis, TN–based company said. The change is to apply to U.S. domestic and export express package and freight shipments.
Source: http://biz.yahoo.com/ap/061103/fedex_rates.html?v=1
20. *November 03, DM News* — **USPS encourages mailers to use electronic documentation.** The U.S. Postal Service (USPS) is making every effort to help its 2.5 million business mail customers switch from hardcopy postage statements to a seamless, electronic acceptance method designed to improve efficiency and maximize ease. According to an announcement made at the quarterly Mailers Technical Advisory Committee meeting at postal headquarters, all business customers — small, medium and large — can now submit postage statements electronically and gain online access to postal accounts in PostalOne, 24 hours a day, seven days a week. "By encouraging the electronic submission of postage documents and providing online access to permit and account information, the postal service is working to meet the growing business needs of its customers," said Susan Plonkey, vice president of customer service for the USPS. PostalOne is an electronic suite of services that links a customer's mailing information electronically with USPS acceptance, verification and payment systems, eliminating most of the paperwork. Large business mailers previously used the system.
Source: <http://www.dmnews.com/cms/dm-news/direct-mail/38846.html>

[\[Return to top\]](#)

Agriculture Sector

21. *November 02, Animal and Plant Health Inspection Service* — **USDA seeks comments on three petitions regarding delayed implementation of chronic wasting disease regulations.** The U.S. Department of Agriculture's (USDA) Animal and Plant Health Inspection Service (APHIS) is soliciting comments on three petitions requesting that APHIS reconsider provisions and delay a recent final rule establishing a herd certification program and interstate movement restrictions for cervids to control the spread of chronic wasting disease (CWD). The CWD herd certification program and interstate movement of farmed or captive deer, elk and moose final rule, published on July 21, originally had an effective date of October 19. However, in early August, APHIS received petitions from the Association of Fish and Wildlife Agencies, the National Assembly of State Animal Health Officials and the United States Animal Health Association asking for a delay and review. APHIS is taking this opportunity to solicit comments on the merits of these three petitions.
Source: <http://www.aphis.usda.gov/newsroom/content/2006/11/cwdpetit.shtml>
22. *November 02, KTRV-TV (ID)* — **Elk herd testing in Idaho.** The Idaho Department of Agriculture has gotten test results back from elk that escaped from a private hunting reserve in eastern Idaho. In all, 36 elk were killed under the direction of Idaho Fish and Game, who feared the escaped animals might interbreed and cause disease among native elk. Of the 19 sampled for red deer trait, 12 came back negative. Twenty–two were tested for chronic wasting disease,

20 were negative. Also, 25 of the 26 sampled for brucellosis tested negative as well.

Source: <http://www.fox12news.com/Global/story.asp?S=5628226>

23. *November 02, Associated Press* — Testing confirms fish disease in eastern Lake Erie.

Testing in New York has confirmed a deadly disease among fish in eastern Lake Erie following an outbreak of the virus in Lake Ontario and the Saint Lawrence River. New York's Department of Environmental Conservation says viral hemorrhagic septicemia (VHS) doesn't pose any threat to humans, but has been blamed for killing off large numbers of fish in the Great Lakes region. The virus has been confirmed in nine species of fish, including rock bass and smallmouth bass.

Source: http://www.wkyc.com/news/news_article.aspx?storyid=58781

24. *November 02, Virginia Tech Collegiate Times (VA)* — Virginia Tech teams up with the Department of Homeland Security.

Virginia Tech has joined several other universities to develop a program funded by the Department of Homeland Security to train small agricultural communities to detect areas of food supply and transportation that are vulnerable to attacks of terrorism. "A lot of people don't realize that veterinary medicine plays a critical role in national security," said Jeffrey Douglas, college communication manager for University Relations. "In this post 9/11 world we live in, the dangers of a terrorist entity contaminating our food supplies are real, and if you ever stop to think about it, the economic consequences of shutting down a food production network can be devastating." The purpose of this project, called Agricultural Vulnerability Assessment Training Program, is to develop classroom like training sessions that will give farmers and producers the tools to detect areas of vulnerability in food production, packaging and transportation, and also teach them how to restore economic order in case of an attack. The program will be presented in 34 different locations throughout the United States.

Source: <http://www.collegiatetimes.com/news/1/ARTICLE/7932/2006-11-02.html>

[[Return to top](#)]

Food Sector

25. *November 03, U.S. Food and Drug Administration* — FDA says tomatoes in restaurants linked to Salmonella Typhimurium outbreak.

The U.S. Food and Drug Administration (FDA) announced Friday, November 3, the results of an investigation by state and Centers for Disease Control and Prevention (CDC) investigators, which found consuming tomatoes in restaurants as the cause of illnesses in the Salmonella Typhimurium outbreak. To date, 21 states have reported 183 cases of illnesses to the CDC. Based on information currently available from the CDC, the investigation shows a peak in cases of illness in late September. This suggests that the outbreak is not ongoing. The agency believes that the tomatoes that caused the illnesses have at this point been consumed, destroyed or thrown out because they are perishable. Therefore, FDA does not believe a consumer warning about tomatoes on store shelves is warranted at this time. FDA has initiated a traceback of these tomatoes and continues its close collaboration with the CDC and state and local authorities to identify the source of contamination on tomatoes in this outbreak. In particular, FDA is working closely with the states of Minnesota, Massachusetts, and Connecticut, since groups of illnesses were specifically reported in these states.

Source: <http://www.fda.gov/bbs/topics/NEWS/2006/NEW01504.html>

[\[Return to top\]](#)

Water Sector

Nothing to report.

[\[Return to top\]](#)

Public Health Sector

26. *November 03, HealthDay News (CT)* — Flu's misery may lie in the genes: study. A new study of flu-infected mice found that certain genes spurred a strong immune response in the lungs that led to much more severe illness. Mice that didn't exhibit such an immune response were more likely to recover, the researchers found. The findings may help humans not only survive the annual flu season but also an avian flu pandemic, should it ever arise. "The long-term implications would fit into the idea of genetically based preventive medicine," explained co-researcher Dr. Linda Toth, associate dean of research at Southern Illinois University School of Medicine in Springfield. "To know that some people are predisposed to any kind of disease, we would be able to better advise or monitor those people so as to limit their health risk." This knowledge might also help public health officials allocate precious resources. She and co-researcher Rita Trammell, an assistant professor of internal medicine at Southern Illinois University School of Medicine, presented the findings Friday, November 3, at a meeting of the American Physiological Society, in Fort Lauderdale, FL.

Source: <http://www.healthday.com/view.cfm?id=535900>

27. *November 02, Times of India* — Mystery fatal disease in Nepal diagnosed. The mystery disease that has spread in some villages of Banke district in mid-western Nepal for the past two weeks was diagnosed as cerebral malaria, The Himalayan Times reported on Thursday, November 2. Fifteen of the patients were found infected with malaria and as many as 36 people have died of the "unknown" disease that has spread in six villages in Banke district.

Source: <http://timesofindia.indiatimes.com/articleshow/291259.cms>

28. *November 02, Center for Infectious Disease Research & Policy (MN)* — WHO report calls H5N1 vaccine stockpiling premature. A group of influenza experts convened by the World Health Organization (WHO) cautioned Thursday, November 2, that governments shouldn't stockpile "pre-pandemic" H5N1 influenza vaccines now, because too little is known about the requirements for an effective vaccine. The group of 22 scientists, who met for 2 days in September, "agreed that governments should not rush to place orders for pre-pandemic vaccines when so many fundamental scientific questions are still outstanding," says their report. Some other observations and recommendations in the wide-ranging report are as follows: a) A simple, rapid, and reliable diagnostic test for use in the field and at the patient's bedside is urgently needed; b) Research is needed to determine what makes children and young adults especially vulnerable to infection; c) Studies are needed to determine if a genetic predisposition increases the risk of human infection or of human-to-human transmission among blood relatives.

WHO report: <http://www.who.int/csr/resources/publications/influenza/WHO>

29. *November 02, Reuters* — **Study points to migrating ducks in bird flu spread.** Migrating ducks, geese, and swans spread the H5N1 bird flu virus from Russia to Romania, Turkey and Ukraine, researchers said on Thursday, November 2. A careful analysis of the spread of the virus from central Asia into eastern Europe in the autumn of 2005 shows that wild birds, especially mallard ducks, were the chief spreaders of the virus. "We conclude that the spread of (highly pathogenic avian influenza) H5N1 virus from Russia and Kazakhstan to the Black Sea basin is consistent in space and time with the hypothesis that birds in the Anatidae family have seeded the virus along their autumn migration routes," the researchers wrote in the journal *Emerging Infectious Diseases*. Anatidae include geese, ducks and swans, some of which are killed by H5N1, and other species of which often show no ill effects from the virus but which can spread it. Mallard ducks are the main suspect.
Study: <http://www.cdc.gov/ncidod/EID/vol12no11/06-0223.htm>
Source: <http://www.alertnet.org/thenews/newsdesk/N02387076.htm>

30. *November 02, University at Buffalo (NY)* — **Legal preparedness essential for public health emergencies.** In the event of an emergency or disaster, an array of legal issues will arise affecting the speed and effectiveness of emergency response. And when a crisis occurs across borders, international legal obligations and restraints present challenges that can further affect emergency response. This is why "legal preparedness" is key among many factors essential to an effective emergency response, explains Sheila Shulman, research associate professor in the University at Buffalo Law School and the School of Public Health and Health Professions in New York. "Public health officials, health care providers, private entities, institutions and corporations, as well as the broader community need a clear and fundamental understanding of basic public health law, clarity about the broader legal obligations and constraints that will govern in the event of a community crisis, and recognition of the complex ethical challenges that inevitably will emerge," Shulman says. To address these issues, the Baldy Center for Law and Social Policy will hold a day-long public symposium Friday, November 17, on "Public Health Emergencies and Legal Preparedness: A Cross-Border Challenge." The symposium is intended for public health officials, health law attorneys, hospital and corporate risk managers, and law enforcement personnel.
Source: <http://www.buffalo.edu/reporter/vol38/vol38n10/articles/BaldyConf.html>

[\[Return to top\]](#)

Government Sector

31. *November 03, National Journal's Technology Daily* — **DHS eyes data fusion in states, localities.** The Department of Homeland Security (DHS) hopes to improve information sharing with state and local government fusion centers by giving those centers intelligence officers and an advanced communications network for classified information, a senior official said Friday, November 3. Department Chief Intelligence Officer Charles Allen said he plans to have intelligence officers embedded at 18 fusion centers by the end of fiscal 2007 and at all other centers by the end of fiscal 2008. Fusion centers are central locations where local, state and federal officials work to receive, integrate and analyze intelligence. Allen said he already has

deployed officers to centers in Atlanta; Baltimore; Baton Rouge, LA; Los Angeles; and New York. He said more officers will be deployed to centers in Arizona, California, Florida, Illinois, New York, Texas, and Virginia by January. State and local governments have said lack of access to classified information on a routine basis at fusion centers is a major problem. Allen said he plans to address that problem through better use of information technology.

Source: <http://www.govexec.com/dailyfed/1106/110306tdpm1.htm>

[[Return to top](#)]

Emergency Services Sector

32. *November 03, Daily Item (PA)* — New emergency software for Union County,

Pennsylvania. Emergency officials in Union County, PA, will soon launch a state-of-the-art computer software program designed to further enhance emergency tactical operations in the county. The software, already in use in California, will be incorporated at the soon-to-be new communications center at the Union County Government Center in Lewisburg and on location at the former Laurelton Center. "The software package will enable us to reach other data sources and give the responders in the field ability to make immediate decisions in response to an emergency," said Tom Hess, director of Union County emergency management. He added that the process is currently done by radio communication. "The dispatcher and responders in the field will have access to the same data at the same time." The county continues its work on upgrading the current system and setting up the new center. Hess said that the majority of the communications equipment has been ordered and that the initial phase of installation will begin later this month. "When we are done, we will have the newest equipment and increased ability to manage emergencies, including the ability to locate wireless 911 calls," Hess said.

Source: <http://www.dailyitem.com/apps/pbcs.dll/article?AID=/20061103/NEWS/611030310>

33. *November 02, Federal Emergency Management Agency* — President declares major disaster for Louisiana. The head of the U.S. Department of Homeland Security's Federal Emergency Management Agency (FEMA) announced Thursday, November 2, that federal disaster aid has been made available for the state of Louisiana to help people and communities recover from the effects of severe storms and flooding beginning on October 16, 2006, and continuing. FEMA Director David Paulison said the assistance was authorized under a major disaster declaration issued for the state by President Bush. The President's action makes federal funding available to affected individuals in the parishes of Caldwell, Franklin, Grant, LaSalle, Madison, Morehouse, Natchitoches, Richland, Sabine, Vernon and Winn. The assistance, to be coordinated by FEMA, can include grants to help pay for temporary housing, home repairs and other serious disaster-related expenses. Low-interest loans from the U.S. Small Business Administration also will be available to cover residential and business losses not fully compensated by insurance.

Source: <http://www.fema.gov/news/newsrelease.fema?id=31223>

34. *November 02, Federal Emergency Management Agency* — President declares major disaster for Missouri. The head of the U.S. Department of Homeland Security's Federal Emergency Management Agency (FEMA) announced Thursday, November 2, that federal disaster aid has been made available for Missouri to supplement state and local recovery efforts in the area struck by severe storms during the period of July 19–21, 2006. FEMA Director David Paulison

said federal funding is available to state and eligible local governments and certain private nonprofit organizations on a cost-sharing basis for emergency work and the repair or replacement of facilities damaged by the severe storms in the independent city of St. Louis. Source: <http://www.fema.gov/news/newsrelease.fema?id=31224>

[\[Return to top\]](#)

Information Technology and Telecommunications Sector

35. *November 03, IDG News Service* — **Security threat changing, says Symantec CEO.** The threat posed to computer users and companies by hackers is shifting from attacks on the computers to attacks on electronic transactions, according to the head of one of the world's largest security software vendors. John Thompson, chairman and CEO of Symantec, said the change has been taking place over the last few years but has recently been accelerating. "The attacks that we see today are more targeted and more silent and their objective is to create true financial harm as opposed to visibility for the attackers," he said. The head of Symantec's Asia Pacific business, Bill Robbins, explained in an interview that this changing threat would mean businesses will have to spend more time and energy on making sure that data is not just secure but also recording which users are accessing and manipulating information stored in corporate databases. Source: http://www.infoworld.com/article/06/11/03/HNchangingsecurity_threat_1.html
36. *November 03, IDG News Service* — **FTC settles with adware company.** Adware distributor Zango will give up \$3 million in "ill-gotten gains" for deceptive downloads that displayed billions of unwanted pop-up ads in a settlement with the U.S. Federal Trade Commission (FTC). The settlement, announced Friday, November 3, bars Zango from loading software onto consumers' computers without their consent, the FTC said. The settlement also requires Zango, formerly known as 180solutions, to provide a way for consumers to remove the adware. FTC settlement: <http://www.ftc.gov/os/caselist/0523130/0523130agree061103.pdf> Source: http://www.infoworld.com/article/06/11/03/HNftcadware_1.html
37. *November 03, VNUNet* — **Hackers use Wikipedia to spread malware.** Hackers are using online encyclopedia Wikipedia to spread malware, according to a security firm. Sophos discovered that hackers had created an article on the German edition of Wikipedia containing false information about a new version of the Blaster worm, along with a link to a fix. However, the fix is actually a piece of malicious code designed to infect visitors' PCs. Wikipedia is built from user contributions, allowing anyone to create or edit the content of a page. The hackers sent spam messages to German computer users, which purported to come from Wikipedia, and directed recipients to the fraudulent information. As the e-mails linked to a legitimate Website, they were able to bypass some anti-spam solutions. Source: <http://www.vnunet.com/vnunet/news/2167949/hackers-wikipedia-dupe-users>
38. *November 02, Security Focus* — **Microsoft Internet Explorer MHTML denial-of-service vulnerability.** Microsoft Internet Explorer is prone to a denial-of-service vulnerability. This issue occurs when Internet Explorer attempts to parse certain malformed HTML content. Successfully exploiting this issue will cause the affected application to crash, denying service to

legitimate users. Internet Explorer 7 is vulnerable to this issue; other versions may also be affected.

Solution: Currently, Security Focus is not aware of any vendor-supplied patches for this issue.

Source: <http://www.securityfocus.com/bid/20875/references>

39. *November 02, National Journal* — **Agencies close to satisfying cybersecurity law.** The White House Office of Management and Budget (OMB) predicts that the percentage of federal systems complying with a 2004 law requiring agencies to identify cyber risks and develop ways to combat them will be up next year. Karen Evans, OMB's administrator of e-government and information technology, told a cybersecurity conference Thursday, November 2, that early numbers based on reports submitted October 1 show that 88 percent of systems will meet certification and accreditation. That is up from 85 percent last year. She said the number of systems with tested contingency plans is expected to be 78 percent, compared with 60 percent in 2005.

Source: [http://www.govexec.com/story_page.cfm?articleid=35402&dcn=to daysnews](http://www.govexec.com/story_page.cfm?articleid=35402&dcn=to%20daysnews)

Internet Alert Dashboard

Current Port Attacks	
Top 10 Target Ports	15281 (---), 1026 (win-rpc), 6881 (bittorrent), 4662 (eDonkey2000), 1027 (icq), 4672 (eMule), 1028 (---), 50001 (---), 38973 (---), 25 (smtp)
Source: http://isc.incidents.org/top10.html ; Internet Storm Center	
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov .	
Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it-isac.org/ .	

[\[Return to top\]](#)

Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

[\[Return to top\]](#)

General Sector

Nothing to report.

[\[Return to top\]](#)

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.